Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE DIVISION OF INFORMATION RESOURCES MANAGEMENT'S OPERATING SYSTEM (MVS) AND ACCESS CONTROL SOFTWARE (CA-ACF2)

OFFICE OF INSPECTOR GENERAL

(A9606) **July 1996**

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

July 1996

Mr. Stephen R. Malphrus, Director
Division of Information Resources Management

We are pleased to present our final *Report on the Audit of the Division of Information Resources Management's Operating System (MVS) and Access Control Software (CA-ACF2)* (A9603). We performed this audit to determine if the operating system has an adequate level of internal controls and that the access control software has been implemented and maintained in a manner that ensures adequate access control to the MVS operating system and the Board's computer resources.

Overall, we believe that controls over the Board's operating system and access control software need to be strengthened. We found insufficient controls over system programmer access to the production operating system's libraries and data, insufficient audit trails, and inadequate separation of duties among your staff. We also found that controls over the options settings for the access control software do not ensure that these settings are current and that they adequately control the Board's mainframe system software products. Our report contains two recommendations that are designed to enhance access control and maintenance procedures, which we believe are the systemic causes for the control weaknesses we found.

We provided a draft of this report for you and your staff's review and comment. Your response indicates only partial concurrence with our two recommendations. Specifically, you plan to strengthen access control by restricting update authority to the production MVS operating system and the CA-ACF2 security rules database to the three system programmers who have primary responsibility for the maintenance of the operating system, and by logging their access. As discussed in our analysis of comments, we continue to question the need for ongoing update access to the CA-ACF2 security rules database by these systems programmers to effectively maintain the operating system. We checked and found that no updates were performed by these systems programmers on the CA-ACF2 rules database during the last six months and thus we believe restricting their access authority would be more appropriate to promote adequate separation of duties.

A copy of this report is being sent to the Administrative Governor and to the Staff Director for Management. The report is available to the public, and a summary will appear in our next semiannual report to Congress. We plan to follow-up on implementation of our recommendations and will report any exceptions as part of our future audit activities.

Sincerely,

Barry R. Snyder
Assistant Inspector General for Audits

Enclosure

TABLE OF CONTENTS

Page

BACKGROUND

The Board of Governors of the Federal Reserve System (the Board) relies heavily on its mainframe computer system to process and analyze data used in making monetary and economic policy decisions and in performing its other regulatory, operational, and administrative activities. Some of the more important mainframe applications that the Board uses in fulfilling its mission include

— the Banking Statistics Standard Application (STAT), which processes and edits the majority of the economic data series used within the Federal Reserve System;

— the National Information Center (NIC), which provides the Federal Reserve System with a database containing information on the organizational structure, financial condition, and supervisory evaluation of the nation's bankholding companies and their nonbank subsidiaries, banks, and other financial institutions;

— the Home Mortgage Disclosure Act (HMDA) System, which maintains a centralized database recording the race, sex, and income for mortgage applicants of most financial institutions;

— the Currency Shipment and Ordering System (CASH), which monitors and controls the production and distribution of newly printed currency between the Bureau of Engraving and Printing and the Federal Reserve Banks and their Branches; and

— the Administrative Information Retrieval System (AIRS), which processes the Board's payroll and personnel information, including employment, compensation, and benefits data.

These and other mainframe applications need to operate in a secure and reliable processing environment. Two critical pieces of software that affect the integrity and security of this environment are the operating system and the access control software. The Board's mainframe uses the Multiple Virtual Storage (MVS) operating system, a complex, integrated set of system software that supervises the sequencing and processing of applications, allocates storage and central processors, and assigns file disk space. In addition, MVS facilitates the sharing of computer hardware and software and assures system integrity by isolating and protecting applications and other software. The Board also uses Computer Associates Access Control Facility (CA-ACF2), which operates as an extension of the MVS operating system, to protect application programs and data against unapproved destruction, modification, or disclosure. CA-ACF2 identifies and authenticates users when they access the computer; protects programs and data by defining, through a set of rules, who can use the programs

computers. These manuals were published in 1995, but full compliance is not required until January 1997.

OBJECTIVES, SCOPE, AND METHODOLOGY

We performed an audit of the Board's MVS mainframe operating system and CA-ACF2 access control software to evaluate the security and integrity of their installation and maintenance. Specifically, we wanted to determine if (1) the operating system has an adequate level of internal controls and (2) the access control software has been implemented and maintained in a manner that ensures adequate access control to the MVS operating system and the Board's computer resources. To accomplish these objectives, we reviewed policies, procedures, and technical documentation related to the installation and maintenance of the two software systems. We also used CA-EXAMINE, one of Computer Associates' technical tools, to determine whether the installation, modification, and maintenance of the operating system complies with the Federal Reserve's security guidelines and system integrity requirements. We also reviewed the installation settings for the CA-ACF2 system options to evaluate the level of security they provide and to determine the reasonableness of the installed options. Our audit was performed from January 1996 to March 1996 and was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Overall, we believe that controls over the Board's MVS operating system and CA-ACF2 access control software need to be strengthened. Specifically, we found insufficient controls over system programmers' access to the production operating system's libraries and data, incomplete audit trails for monitoring the modification and maintenance of the operating system by system programmers, and inadequate separation of duties among IRM staff. We also found that the controls over the CA-ACF2 option settings do not ensure that these settings are current and that they adequately control the mainframe system software products. In all, twenty specific control weaknesses were found in reviewing the operating system and access control software. We provided these technical findings, along with specific recommendations for corrective action, under a separate restricted cover to the Director of IRM for appropriate disposition. This report contains two recommendations that address access control deficiencies and poor maintenance procedures—in our opinion, the two systemic causes for the twenty control weaknesses that we found.

The current practice of providing systems programmers access to the MVS production operating system potentially allows them to circumvent or disable any security mechanism, alter any audit trail, and access or modify production data. Our first recommendation would restrict systems programmers' access to system files to a need-to-know basis, eliminate their access to security and production data, and preserve the integrity of system audit trails. Implementing this recommendation would also address many of the specific control weaknesses reported separately. Our second recommendation would help ensure that CA-ACF2 option settings that bypass data- access rule validation are current and properly controlled. We believe that implementing these recommendations will provide a stronger level of access controls, strengthen the security over the Board's mainframe computer system, and better preserve the integrity of the MVS operating system.

1. We recommend that the Director of IRM restrict systems programmer's access to the MVS production operating system to a need-to-know basis, enforce separation of duties with respect to computer security administration, and maintain adequate audit trails or logs of access to sensitive libraries.

As the software is currently configured, IRM systems programmers have access to the Authorized Program Facility (APF) libraries of MVS. System and/or user programs stored in APF libraries are authorized to use sensitive system functions, including privileged instructions that are generally restricted because they can compromise the security and integrity of the computer. Additionally, authorized programs can access all memory, including system memory and memory assigned to user programs. Essentially, an authorized program can access any real storage on the computer, including production data. With their current access levels, IRM systems programmers could circumvent or disable any security mechanism, alter any audit trail, and access or modify any production data in spite of CA-ACF2 access control software.

According to the System's *Mainframe and FEDNET Security Support Manual*, access to programs in APF libraries should be restricted to authorized personnel based on a person's "need to know," which is defined as the principle of granting access based on job requirements. Therefore, to control these powerful features, the Board can either (1) deny systems programmers ongoing update access to the MVS and APF libraries and grant access only to handle emergencies or other problems or (2) allow systems programmers limited ongoing access on a need-to-know basis and partition job responsibilities to enforce separation of duties. We believe this latter approach would better fit the Board's mainframe environment if coupled with improved separation of duties and improved audit trails.

We also found inadequate separation of duties among systems programmers and between systems programmers and security administrators. For example, the Board's data security

rules currently allow both MVS systems programmers and network systems programmers to access certain network APF libraries rather than limiting access to just the network systems programmers. We also found that systems programmers can update, without authorization, the CA-ACF2 security rules databases to access libraries and data outside their assigned job responsibilities. The rules also allow security administrators to update the MVS catalogs. Based on the Federal Reserve System's *Information Security Manual*, each system software product (that is, MVS and CA-ACF2) should have a designated owner who is responsible for reviewing security features and controlling the receipt, installation, and maintenance of the software.

Additionally, we found that updates to all major MVS and CA-ACF2 libraries are not being uniformly logged and the integrity of the logs currently written is not protected against modification by the systems programmers. Updates of all major MVS system libraries and authorized program libraries should be logged and the logs should be restricted so that access to these sensitive programs can be monitored.

2. We recommend that the Director of IRM develop control procedures over the CA-ACF2 system option settings and periodically review these settings to ensure that they are current and adequate.

Mainframe installations can tailor or customize the use of CA-ACF2 to the individual users, data, and resources in their environment by setting certain options. Many of these option settings authorize programs to bypass CA-ACF2 rule validations, or control sensitive programs that have the capability to bypass rule validation, or enable a user full access to any data or resource despite any data-access security rules to the contrary. We found that many of the CA-ACF2 option settings in the Board's mainframe environment are outdated. They control programs that no longer exist, have been superseded by new software, are incompatible with other settings, are set so they have no effect, grant inappropriate access authority, or are incomplete.

Incorrect CA-ACF2 option settings create security exposures. For example, a program that no longer exists but is still defined to CA-ACF2 as having special security bypass privileges can be replaced by a program with a similar name but a different function and assume the old program's access control bypass capabilities. Our review showed that many of the outdated CA-ACF2 option settings resulted from changes in the Board's systems program products. The Federal Reserve System's *Mainframe and FEDNET Security Support Manual* requires the Board to control and log the use of features that bypass security controls. We believe IRM needs to develop formal procedures for identifying, authenticating, and authorizing these sensitive CA-ACF2 features and needs to periodically review these option settings to ensure that they are current and match the requirements of the Board's system software products.

ANALYSIS OF COMMENTS

We provided a draft copy of this report to the Director of IRM for his response which is included as appendix 1. Regarding the first recommendation, which addresses restricting systems programmer access to the MVS production operating system, enforcing separation of duties, and logging access to sensitive libraries, the director partially concurs and plans to restrict update authority to three systems programmers and log their access. However, he does not believe that additional separation of duties is necessary. We continue to disagree on this point, especially with respect to the system programmers need to have on-going access to the CA-ACF2 security rule databases. We found that the three systems programmers had not used their update access to the security rules database during the last six months, supporting our opinion that on-going access is not required by the systems programmers. Granting access on an emergency basis would enhance separation of duties while not impeding the ability of the systems programmers to perform their functions.

The director also partially agreed with our second recommendation regarding the need to develop control procedures over the CA-ACF2 system option settings and to periodically review the settings to ensure that they are current and adequate. He stated that control procedures already exist and that the settings are periodically reviewed. Furthermore, he believes that the magnitude of the problem was overstated, citing that only a few of the settings were outdated and those were corrected immediately after the division was notified of the problem. We continue to believe that the director should improve controls in this area, given that we had eleven technical findings regarding improper option settings.